CLAIMS

What is claimed is:

1. A method for protecting content in a computing system having an open system architecture and providing the content to an external system, including the steps of:

(a) in a closed subsystem of the computing system, generating raw content by decrypting and optionally performing additional processing on encrypted content;

(b) in the closed subsystem, generating protected content by re-encrypting the raw content; and

(c) asserting the protected content from the closed subsystem to the external system without providing the computing subsystem access to the protected content.

2. The method of claim 1, wherein step (a) includes the steps of:

decrypting the encrypted content to generate decrypted data; and

performing decompression on the decrypted data to generate the raw content.

3. The method of claim 1, wherein the digital video data are high-definition digital video data read from a disk, and step (a) includes the steps of:

decrypting the high-definition digital video data to generate decrypted data; and

performing decompression on the decrypted data to generate raw content.

4. The method of claim 1, wherein the encrypted content comprises digital video data read from a disk.

5. The method of claim 4, wherein the digital video data are high-definition digital video data, and step (b) includes the step of re-encrypting the raw content in accordance with the HDCP protocol.

6. The method of claim 1, also including the step of receiving the encrypted content from a source external to the computing system.

7. The method of claim 1, also including the step of receiving the encrypted content from a source external to the computing system via the internet.

8. A computing system having an open system architecture, said system including:

a closed subsystem configured to generate protected content; and

a computing subsystem, coupled and configured to generate additional content and to assert the additional content to the closed subsystem,

wherein the closed subsystem has at least one output configured to be coupled to an external system, the closed subsystem is operable in a first mode in which it asserts the protected content to the at least one output, and the closed subsystem is operable in a second mode in which it asserts the additional content to the at least one output.

9. The system of claim 8, wherein the protected content comprises encrypted high-definition digital video data.

10. The system of claim 8, wherein the protected content and the additional content are audiovisual data.

11. The system of claim 8, wherein the closed subsystem is operable in the first mode to assert the protected content to the at least one output without providing the computing subsystem access to the protected content.

12. The system of claim 11, wherein the closed subsystem is also operable in the first mode to assert key data or authentication data to the at least one output without providing the computing subsystem access to the key data or authentication data.

13. The system of claim 8, also including the external system, wherein the protected content comprises encrypted video data, and wherein said external system includes:

at least one input coupled to the at least one output of the closed subsystem; and

decryption circuitry, coupled to the at least one input and configured to generate display data by decrypting the encrypted video data.

14. The system of claim 13, wherein the display data are high-definition digital video data.

15. The system of claim 8, also including the external system, wherein said external system is a closed audiovisual system having at least one input coupled to the at least one output of the closed subsystem.

16. The system of claim 8, also including the external system, wherein said external system has at least one input coupled to the at least one output of the closed subsystem and comprises a high-definition digital video monitor and at least one loudspeaker.

17. The system of claim 8, also including the external system, wherein said external system has at least one input coupled to the at least one output of the closed subsystem and comprises a digital video monitor.

18. The system of claim 8, wherein the closed subsystem comprises an HD-DVD drive configured to decrypt high-definition digital video read from a disk to generate decrypted data, to perform decompression on the decrypted data to generate raw content, and to generate the protected content by re-encrypting the raw content.

19. The system of claim 18, wherein the closed subsystem is configured to re-encrypt the raw content in accordance with the HDCP protocol.

20. The system of claim 8, wherein the closed subsystem includes an HD-DVD drive, said HD-DVD drive including:

a multiplexer having a first output, a second output, and an input coupled to receive digital data read from a disk, wherein the digital data include non-protected data and other data, and the multiplexer is operable to assert the non-protected data to the first output and to assert the other data to the second output;

first circuitry coupled to the first output of the multiplexer; and

second circuitry coupled to the second output of the multiplexer, wherein the first circuitry is configured to assert data indicative of the non-protected data to the computing system, and the second circuitry is configured to generate the protected content in response to the other data.

21. The system of claim 20, wherein the second circuitry is configured to decrypt the other data to generate decrypted data, to perform decompression on the decrypted data to generate raw content, and to generate the protected content by re-encrypting the raw content.

22. The system of claim 20, wherein the second circuitry is configured to perform the re-encryption in accordance with the HDCP protocol.

23. The system of claim 8, wherein the closed subsystem includes additional circuitry coupled between the at least one output and the computing subsystem, and the additional circuitry has a first state in which it asserts the protected content to the at least one output and a second state in which it asserts the additional content from the computing subsystem to the at least one output.

24. The system of claim 23, wherein the computing subsystem includes:

a CPU;

a graphics controller, coupled between the CPU and the additional circuitry, and wherein the graphics controller is configured to assert the additional content to the closed subsystem; and

an I/O controller, coupled between the graphics controller and the closed subsystem and configured to control at least one operation of the closed subsystem.

25. The system of claim 23, wherein the additional circuitry is a switch having an input coupled to receive the additional content, another input coupled to receive the protected content, and a switch output coupled to the at least one output of the closed subsystem.

26. A computing system having an open system architecture, said system including:

a closed subsystem, configured to decrypt encrypted content to generate raw content and to generate protected content by re-encrypting the raw content; and a computing subsystem configured to generate additional content,

wherein the closed subsystem has at least one output configured to be coupled to an external system, and the closed subsystem is operable to assert the protected content to the at least one output.

27. The system of claim 26, wherein the raw content comprises high-definition digital video data.

28. The system of claim 26, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

29. The system of claim 28, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content.

30. The system of claim 29, wherein the closed subsystem is operable in a first mode in which it asserts the protected content to the at least one output, and the closed subsystem is operable in a second mode in which it asserts the additional content to the at least one output.

31. A computing system having an open system architecture, said system including:

a closed subsystem configured to decrypt encrypted content to generate decrypted data, to perform decompression on the decrypted data to generate raw content, and to generate protected content by re-encrypting the raw content; and

a computing subsystem configured to generate additional content,

wherein the closed subsystem has at least one output configured to be coupled to an external system, and the closed subsystem is operable to assert the protected content to the at least one output.

32. The system of claim 31, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

33. The system of claim 32, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content.

34. The system of claim 33, wherein the closed subsystem is operable in a first mode in which it asserts the protected content to the at least one output, and the closed subsystem is operable in a second mode in which it asserts the additional content to the at least one output.

35. A computing system having an open system architecture, said system including:

a closed subsystem configured to generate protected content; and

a computing subsystem configured to generate additional content,

wherein the closed subsystem has at least one output configured to be coupled to an external system, the closed subsystem includes combining circuitry coupled between the at least one output and the computing subsystem, and the combining circuitry includes:

a receiver coupled to receive the protected content and configured to decrypt the protected content thereby generating decrypted content; and

additional circuitry having at least one input and at least one additional input, wherein the at least one input is coupled to the computing subsystem to receive the additional content, the at least one additional input is coupled to receive the decrypted content, and the additional circuitry also includes circuitry for performing at least one operation on the decrypted content to generate processed data, and

wherein the additional circuitry is operable to assert output data to the at least one output in a first state and in a second state, wherein the output data asserted by the additional circuitry in the first state are the processed data, and the output data asserted by the additional circuitry in the second state are the additional content.

36. A computing system having an open system architecture, said system including:

a closed subsystem configured to generate protected content by encrypting raw content; and a computing subsystem coupled to the closed subsystem but having no access to the raw content, wherein the computing subsystem has at least one output configured to be coupled to an external system,

wherein the computing subsystem is operable in a first mode in which it receives the protected content from the closed subsystem and asserts the protected content to the at least one output, and the computing subsystem is operable in a second mode in which it asserts other content to the at least one output.

37. The system of claim 36, wherein the protected content comprises encrypted high-definition digital video data.

38. The system of claim 36, wherein the protected content and the other content are audiovisual data.

39. The system of claim 36, also including the external system, wherein the protected content comprises encrypted video data, and wherein said external system includes:

at least one input coupled to the at least one output of the computing subsystem; and

decryption circuitry, coupled to the at least one input and configured to generate display data by decrypting the encrypted video data.

40. The system of claim 39, wherein the display data are high-definition digital video data.

41. The system of claim 36, also including the external system, wherein said external system is a closed audiovisual system having at least one input coupled to the at least one output of the computing subsystem.

42. The system of claim 36, also including the external system, wherein said external system has at least one input coupled to the at least one output of the computing subsystem and comprises a high-definition digital video monitor and at least one loudspeaker.

43. The system of claim 36, also including the external system, wherein said external system has at least one input coupled to the at least one output of the closed subsystem and comprises a digital video monitor.

44. The system of claim 36, wherein the closed subsystem is configured to decrypt encrypted content to generate the raw content, and to generate the protected content by re-encrypting the raw content.

45. The system of claim 44, wherein the raw content comprises high-definition digital video data.

46. The system of claim 44, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

47. The system of claim 46, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content

48. The system of claim 36, wherein the closed subsystem is configured to decrypt encrypted content to generate decrypted data, to perform decompression on the decrypted data to generate the raw content, and to generate the protected content by re-encrypting the raw content.

49. The system of claim 48, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

50. The system of claim 49, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content

51. The system of claim 36, wherein the computing subsystem includes:
a CPU;

an HDMI transmitter, having at least one input, and operable in the first mode to assert the protected content to the at least one output of the computing subsystem;

a graphics controller, coupled to the CPU and to the at least one input of the HDMI transmitter; and

an I/O controller, coupled between the graphics controller and the closed subsystem, and configured to control at least one operation of the closed subsystem and to receive the protected content from the closed subsystem.

52. The system of claim 36, wherein the closed subsystem includes an HD-DVD drive configured to decrypt high-definition digital video read from a disk to generate decrypted data, to perform decompression on the decrypted data to generate the raw content, and to generate the protected content by re-encrypting the raw content.

53. The system of claim 52, wherein the closed subsystem is configured to re-encrypt the raw content in accordance with the HDCP protocol.

54. The system of claim 36, wherein the closed subsystem includes an HD-DVD drive, said HD-DVD drive including:

a multiplexer having a first multiplexer output, a second multiplexer output, and an input coupled to receive digital data read from a disk, wherein the digital data include non-protected data and other data, and the multiplexer is operable to assert the non-protected data to the first multiplexer output and to assert the other data to the second multiplexer output;

first circuitry coupled to the first multiplexer output; and

second circuitry coupled to the second multiplexer output and to the first circuitry, wherein the first circuitry is configured to assert data indicative of the non-protected data to the computing subsystem, the second circuitry is configured to generate the protected content in response to the other data and to assert the protected content to the first circuitry, and the first circuitry is configured to assert data indicative of the protected content to the computing subsystem.

55. The system of claim 54, wherein the second circuitry is configured to decrypt the other data to generate decrypted data, to perform decompression on the

decrypted data to generate raw content, and to generate the protected content by re-encrypting the raw content.

56. The system of claim 55, wherein the second circuitry is configured to re-encrypt the raw content in accordance with the HDCP protocol.

57. A disk drive for use with a computing system having an open system architecture, said disk drive including:

a drive controller having a controller output and configured to assert digital data at the controller output, said digital data including non-protected data and other data;

a multiplexer having an input coupled to the controller output for receiving the digital data, said multiplexer also having a first multiplexer output and a second multiplexer output;

a serial interface, having an input coupled to the first multiplexer output; and

additional circuitry, having an input coupled to the second multiplexer output,

wherein the multiplexer is operable to assert the non-protected data to the first multiplexer output and to assert the other data to the second multiplexer output, the serial interface is configured to output data indicative of the non-protected data, and the additional circuitry is configured to generate protected content in response to the other data.

58. The disk drive of claim 57, wherein the additional circuitry includes a second serial interface, and the additional circuitry is configured to assert the protected content at the second serial interface.

59. The disk drive of claim 58, wherein the serial interface is a SATA interface and the second serial interface is an HDMI interface.

60. The disk drive of claim 57, wherein the other data are digital video data.

61. The disk drive of claim 57, wherein the additional circuitry is configured to decrypt the other data to generate decrypted data, to perform decompression on the decrypted data to generate raw content, and to generate the protected content by re-encrypting the raw content.

62. The disk drive of claim 61, wherein the additional circuitry is configured to re-encrypt the raw content in accordance with the HDCP protocol.

63. The disk drive of claim 57, wherein said disk drive is an HD-DVD disk drive.

64. The disk drive of claim 57, wherein the serial interface also has a second input, the additional circuitry is coupled and configured to assert the protected content to the second input of the serial interface, and the serial interface is configured to operate in a first mode in which it outputs the data indicative of the non-protected data and in a second mode in which it outputs data indicative of the protected content.

65. The disk drive of claim 64, wherein the serial interface is a SATA interface.

66. A closed system configured to be embedded in an open computing system, as a closed subsystem of the open computing system, said closed system including:

content generation circuitry configured to decrypt encrypted content to generate raw content, and to generate protected content by re-encrypting the raw content; and

combining circuitry having at least one first input configured to be coupled to receive the protected content from the content generation circuitry, at least one additional input configured to be coupled to the open computing system to receive audiovisual data from said open computing system, and at least one output,

wherein the combining circuitry is operable in a first mode in which it asserts the protected content to the at least one output when the first input is coupled to receive the protected content, and in a second mode in which it asserts the audiovisual data to the at least one output when the at least one additional input is coupled to receive the audiovisual data.

67. The closed system of claim 66, wherein the protected content comprises encrypted video data.

68. The closed system of claim 67, wherein the content generation circuitry includes an HDMI interface, and each said first input of the combining circuitry is configured to be coupled to the HDMI interface to receive the protected content.

69. A closed system configured to be embedded in an open computing system, as a closed subsystem of the open computing system, said closed system including:

content generation circuitry configured to generate raw content by decrypting and optionally performing additional processing on encrypted content, and to generate protected content by re-encrypting the raw content, and including a transmitter configured to assert the protected content; and

combining circuitry including a receiver and having at least one output, wherein the receiver is configured to be coupled to the transmitter to receive the protected content and to decrypt the protected content thereby generating decrypted content, said combining circuitry also including additional circuitry having at least one input and at least one additional input, wherein the at least one input is configured to be coupled to the open computing system to receive audiovisual data, the at least one additional input is coupled to receive the decrypted content, and the additional circuitry also includes circuitry for performing at least one operation on the decrypted content to generate processed data, and

wherein, when the at least one input is coupled to the open computing system and the receiver is coupled to the transmitter, the additional circuitry is operable in a first state to assert the audiovisual data to the at least one output, and in a second state to assert the processed data to the at least one output.

70. The system of claim 69, wherein the transmitter is an HDMI transmitter, and the receiver is an HDMI receiver.

71. The system of claim 70, also including:

a second HDMI transmitter, coupled to the at least one output of the combining circuitry and configured to generate a serial data stream by encrypting the output data.

72. The system of claim 69, wherein the protected content comprises encrypted video data.

73. A computing system having an open system architecture, said system including:

a display device configured to generate decrypted video by decrypting protected content, and to generate a display in response to the decrypted video;

a closed subsystem, configured to generate the protected content; and

a computing subsystem coupled and configured to generate additional content, wherein at least one of the computing subsystem and the closed subsystem is configured to assert the protected content to the display device without providing the computing subsystem with access to a decrypted version of the protected content.

74. The system of claim 73, wherein the protected content comprises encrypted high-definition digital video data.

75. The system of claim 73, wherein the protected content and the additional content are audiovisual data.

76. The system of claim 73, wherein the closed subsystem is configured to decrypt encrypted content to generate raw content, and to generate the protected content by re-encrypting the raw content.

77. The system of claim 76, wherein the raw content comprises high-definition digital video data.

78. The system of claim 76, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

79. The system of claim 78, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content

80. The system of claim 73, wherein the closed subsystem is configured to decrypt encrypted content to generate decrypted data, to perform decompression on the

decrypted data to generate raw content, and to generate the protected content by re-encrypting the raw content.

81. The system of claim 80, wherein the closed subsystem is configured to receive the encrypted content from a remote source.

82. The system of claim 81, wherein the closed subsystem is configured to receive the encrypted content from the remote source via the internet, and the closed subsystem is configured to perform each key exchange and verification operation with the remote source that is needed to accomplish decryption of the encrypted content

83. The system of claim 73, wherein the closed subsystem includes:

combining circuitry, configured to generate combined content by combining the protected content with the additional content, and to assert the combined content to the display device.

84. The system of claim 83, wherein the combining circuitry is configured to generate the combined content by time-division-multiplexing the protected content with the additional content.

85. The system of claim 83, wherein the combining circuitry is configured to generate the combined content by combining the protected content and the additional content such that the display device can display the combined content in a picture-in-picture format.